CLAIMS-

What is claimed is:

1. A method for establishing secure group-based communication comprising:

distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts; and

distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

2. The method as recited in Claim 1 further comprising:

distributing said second set of keys wherein a unique set of keys are distributed to each of said plurality of hosts.

3. The method as recited in Claim 2 further comprising:

distributing said second set of keys wherein each of said plurality of hosts receives a unique key for each of said plurality of hosts except for itself.

4. The method as recited in Claim 1 further comprising:

communicating between said hosts in a utility data center communications environment.

5. The method as recited in Claim 1 further comprising:

authenticating a communication source from a host level.

6. The method as recited in Claim 1 further comprising:

authenticating a communication source from an application level.

7. The method as recited in Claim 1 further comprising:

adding a new host to said plurality of hosts and dynamically modifying said first set of keys in response to adding said new host.

8. The method as recited in Claim 1 further comprising:

in response to removing one of said plurality of hosts, dynamically modifying said first set of keys.

9. The method as recited in Claim 1 further comprising:

dynamically modifying said first set of keys at regular intervals with said second set of keys.

10. A method for establishing a secure group-based communication environment between a plurality of hosts comprising:

distributing a first set of keys to each of said plurality of hosts for encrypting communication between said hosts and for authenticating a source of communication between said plurality of hosts;

distributing a subset of said first set of keys to each of said plurality of hosts for validating said source of communication between said plurality of hosts; and

distributing a second set of keys to each of said plurality of hosts for dynamically modifying said first set of keys and said subset of said first set of keys.

11. The method as recited in Claim 10 further comprising:

adding a new host to said plurality of hosts; and

dynamically modifying said first set of keys and said subset of said first set of keys.

12. The method as recited in Claim 11 further comprising:

dynamically modifying said first set of keys and said subset of said first set of keys with a third set of keys generated in response to adding said new host.

13. The method as recited in Claim 10 further comprising:

removing a host from said plurality of hosts;

dynamically modifying said first set of keys and said subset of said first set of keys.

14. The method as recited in Claim 13 further comprising:

dynamically modifying said first set of keys and said subset of said first set of keys with a third set of keys generated in response to removing said host from said plurality of hosts.

15. The method as recited in Claim 10 further comprising:

communicating between said plurality of hosts in a utility data center communications environment.

16. The method as recited in Claim 10 further comprising:

validating said source of communication between said plurality of hosts at a host level.

17. The method as recited in Claim 10 further comprising:

validating said source of communication between said plurality of hosts at an application level.

18. A computer readable medium comprising executable instructions which, when executed in a processing system, causes the system to perform the steps for a method of establishing secure group-based communication comprising:

distributing a first set of keys to a plurality of hosts for encrypting communication and for source authentication of group-based communication between said plurality of hosts; and

distributing a second set of keys to said plurality of hosts for dynamically modifying said first set of keys.

19. The computer readable medium as recited in Claim 18 wherein said method further comprises:

distributing said second set of keys wherein a unique set of keys are distributed to each of said plurality of hosts.

20. The computer readable medium as recited in Claim 19 wherein said method further comprises:

distributing said second set of keys wherein each of said plurality of hosts receives a unique key for each of said plurality of hosts except for itself.

21. The computer readable medium as recited in Claim 18 wherein said method further comprises:

communicating between said hosts in a utility data center communications environment.

22. The computer readable medium as recited in Claim 18 wherein said method further comprises:

authenticating a communication source from a host level.

23. The computer readable medium as recited in Claim 18 wherein said method further comprises:

authenticating a communication source from an application level.

24. The computer readable medium as recited in Claim 18 wherein said method further comprises:

adding a new host to said plurality of hosts and dynamically modifying said first set of keys in response to adding said new host.

25. The computer readable medium as recited in Claim 18 wherein said method further comprises:

in response to removing one of said plurality of hosts, dynamically modifying said first set of keys.

26. The computer readable medium as recited in Claim 18 wherein said method further comprises:

dynamically modifying said first set of keys at regular intervals with said second set of keys.